International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

An Image Encryption-Then-Compression using clustering and permutation

Er.Ramandeep Kaur[1], Er.Sumeet Kaur[2]

[1]M.Tech Student, Dept.of Computer Engineering, Yadwindra college of Engineering Talwandi Sabo (Bathinda),Punjab,India
[2]Asst.Professor, Dept.of Computer Engineering,Yadwindra college of Engineering Talwandi Sabo(Bahtinda),Punjab,India

---

Abstract - *Data security became the most challenging issue for the IT engineers for the people related to network security. A large no. of methods is used to secure the data but the most common method used to secure the data is encryption process. Encryption can be done on various types of data like text, images and so on. In this paper we are presenting encryption on images. Encryption can be done on the images before sending over the internet.ve have design an algorithm that can perform encryption and compression of images in a single module. Encryption changes the image into other non readable format while compression reduced the size of image so that it became easy to send or receive the images of small size. In this paper we are presenting an ETC system that encrypt and compress the images using clustering and random permutation.*

Encryption is a part of cryptography. So detail study about cryptography is needed. My paper is divided into 4 sections. Section 1 represents Introduction about encryption and various terminologies. Section 2 reviews the previous work done in this field. Section 3 present my algorithm in detail and last section present the summery and results. The proposed algorithm is good in speed and performance as compared to other algorithms. The algorithm can be efficiently used for both lossless and lossy compression.

***Key Words*: Encryption, Decryption, Cryptography method, Data Security**

1.INTRODUCTION

Image encryption is fundamental part of image processing. Securely sending of an image over the internet prevents it from unauthorized access. If a hacker accesses this image then due to encryption he will not be able to decrypt it. So encryption of images is very useful in image security. Encryption can be defined as the process of coveting original data into non-readable format using a key and encryption function is known as encryption. Decryption is a reverse process of encryption. Decryption changes the non-readable format of data into some readable format. The original data is known as plain text while the encrypted data is known as cipher text. The whole process is controlled by some selected piece of information that is known as key. Encryption can be symmetric or asymmetric. In symmetric encryption only one key is used for both encryption and decryption while in asymmetric encryption different keys are used for encryption and decryption. Encryption is a subpart of cryptography.[19][20]

As shown in Fig.(1) suppose the plain text and cipher text are denoted by P and C respectively[9].the encryption process can be shown as C=E Ke(P) where various terms are C=Cipher text, E=Encryption function, Ke=encryption Key and P=Plain text. Similarly decryption process can be calculated as[9] P=D. Kd(C) where various terms are similar to previous process except Kd and D, Kd is a decryption key and D is a decryption function. For symmetric approach Ke=Kd and for asymmetric approach Ke≠Kd.

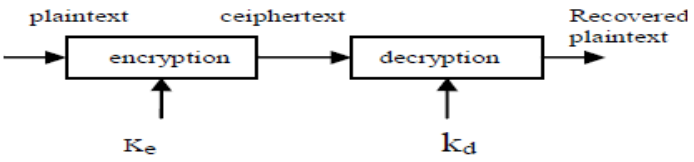


Fig. (1) Encryption Process [19]

For symmetric approach key is kept public. Both sender and receiver know the key. One encrypts the message using that key similarly receiver decrypts the message using same key. The symmetric system is also called public key cryptography. On the other hand in asymmetric key approach two different keys are used for encryption and decryption. The sender encrypts the message using public key that is known to both sender and receiver but the decryption of massage done by the receiver with its own private key that is known only to receiver. Compression reduces the size of image and it can efficiently send over network or store. There is no loss of information in using lossless compression [9].

Now consider an application scenario [19] in which three different people working on image transformation Alice, Bob and Eve. Alice is information owner and wants to securely and efficient transmission of an image [1].Alice is a sender and Bob is receiver. The image transformation takes place using an untrusted channel Eve. Conventionally, this could be done as follows [5].First of all Alice will compress image I into B and to make it non-readable changes it into Ie using an encryption function (Ek) where k stands for secret key as shown in Fig. (2).the encrypted data I(e) forward to Eve and from Eve it simply forward to Bob without any content addition or alteration in message. Receiver simply receives the message and decrypts and decompresses sequentially and got image which is reconstructed. It is called CTE (Compression-then-Encryption) system which is a traditional approach used in this system from long decade.

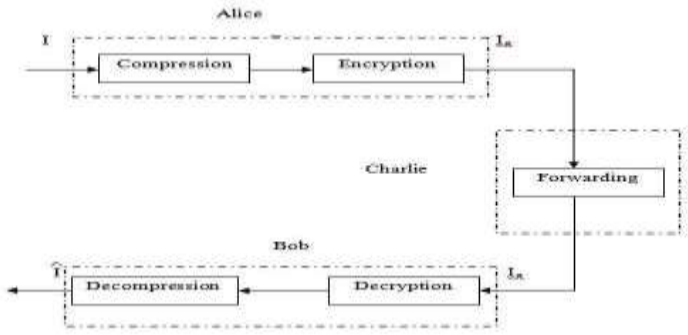


Fig. (2a) Traditional Compression-then-Encryption (CTE)System[19]

Even though the above Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, the order of applying the compression and encryption needs to be reversed in some other situations [3]. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive to compress her data, and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when Alice uses a resource deprived mobile device [1]

In contrast, the channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Charlie, who typically has abundant computational resources. A big challenge within such Encryption-then- Compression (ETC) framework is that compression has to be conducted in the encrypted domain, as Charlie does not access to the secret key K. This type of ETC system is demonstrated in Fig.2 (b) [1].

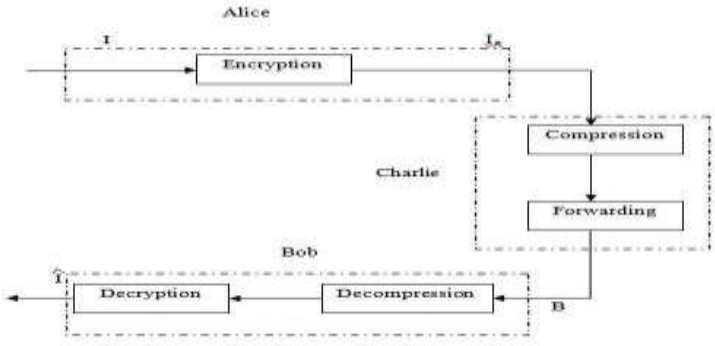


Fig. (2b) Encryption-then-Compression (ETC) System [19]

1.2 Image Compression

It is a process of encapsulate the message to reduce the size of data to sending it easily and efficiently and easy to store. Compression enhances the speed of encryption/decryption. A small bandwidth can use to send a compressed data and utilization of all resources efficiently. Compression can be lossy or lossless. In lossless there is no any loss of data during compression and did not affect the output data. Loss of information is recoverable. On the other hand in lossy compression there is loss of information during compression and can affect result at great extent. Loss of information can never be recovered. Lossless compression is also called reversible and lossy is called non-reversible. On-reversible scheme gives more compression then reversible counterpart [1]. In lossless compression schemes, the reconstructed image, after compression, is numerically identical to the original image [1].lossless compression is used for archival purposes like in medical field, CAD/CAM, Clip art and comic etc. lossy provide more compression ant used at a low data rate. In lossless compression the resulting image is quite similar to input image while in lossy compression the image is more degraded then original image. Lossless method focus on compacting binary data using encoding system [9].lossy encoding methods is varied. And the redundancy produce in image cannot detect by human eye simply.

2. LITERATURE REVIEW

In the literature revive a large no. of papers are studied to examine the previous techniques and their work. The possibility of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years [2]. In Barni method image is divided into various bit plains and by applying LDPC (Low Density parity Check) codes in various bit-planes and exploiting the inter/intra correlation, Lazzeretti and Barni presented several methods for lossless compression of encrypted grayscale/color images [5].ASCII codes are also used to calculate the values of their relevant cipher texts. It is a symmetric data algorithm. It uses only one key for both

encryption and decryption. Key is a major factor in this scheme. It provides speed and unique identification represent by Akanksha Mathur [4].to achieve high compression lossy compression is considered. Data compression is consider for reduce the size of image by reducing the no. of bits in image to transmit it over the network.

A large no. of techniques use key approaches to encryption and decryption process but there is also keyless approaches exist to encrypt the images. The method developed by Pratibha S.Ghode, Abha Gaikwad The method follows SST (Sieving, Shuffling and Transformation) approach for encryption. The input image is divided into pixels and every pixel got encrypted using SST Technique. It gave good quality of output image. It is a secure and efficient technique in image encryption [7]. Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma provide a method based on image bit plain. First of all the grey image is divided into several bit plain images[16].then separately shuffling is done on each bit plain and lastly merge each bit plain to get the encrypted image. The location of each pixel can easily find due to their correlation with neighbor pixel. So the changing of position of pixel not matter at all. The method is popular to encrypt grey images rather than color images.bit plain treated as a single entity and individually shuffled [10].

3. Analysis of Problem

The compression considers for a particular data may be lossless or lossy depend upon the need of user. The main focus of this work on designing a system those provide the facility of encryption and compression in a single module in such a way that compression of encrypted image is equally efficient as original image [2].compression gives better speed due to reduction in data size while encryption provide security to data. So the given method combines the feature of both the approaches to make a secure and efficient system. In the given system encryption can be achieved using predicting error clustering and random permutation and for compression arithmetic coding is used. Furthermore, due to the high sensitivity of prediction error sequence against disturbances, reasonably high level of security could be retained [1].

4. Purposed work

In this section the detail of algorithm is given. It is a three component ETC system that or performed sequentially. First of all the encryption of image takes place that is conduct by Alice. Encryption can be done by using predicting error clustering and random permutation [6]. In next phase compression is done by Eve. Eve performs compression only on encrypted data because he has no right to access key. And at the end decryption and decompression is done by Bob.

4.1. Encryption of image using Predicting error clustering and random permutation

At this part the image is image is divided into a no. of blocks. Each block contains the pixel value for each dot. For each pixel Ii, j we have to calculate predicting error.GAP is use to predict error that defines the best correlation among the pixels. Random error is given as

$$Ei, j=Ii,j - I'I,j$$

The range for predicting error can be [-255,255] and can be mapped to range [0,255].after calculating the error permutation is performed on each block. And each blocks again permutated based on random no.

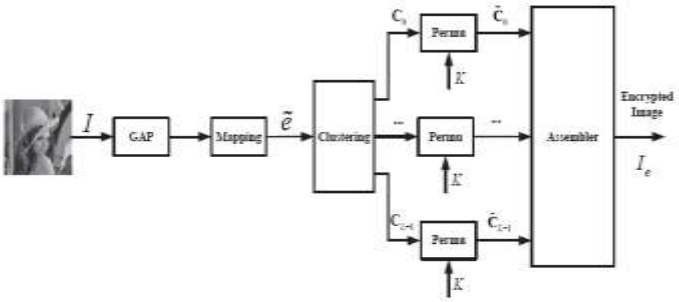


Fig.3- Image encryption using clustering and permutation [1].

Algorithm for this scheme is given below:

1. Compute prediction error for whole image.

2. Divide all prediction errors into L clusters and no. of clusters should be less then L clusters are formed as a result of concatenation of prediction error in a raster scan order [1].

3 now each block rearrange using 2-D block having four columns in each.

4. Perform cyclic shift an each block using a key and read data in raster scan order.

5. At the end all the permutated clusters concatenated using an assembler to get final encrypted image.

4.2.Image compression using AC(Arithmetic Coding)

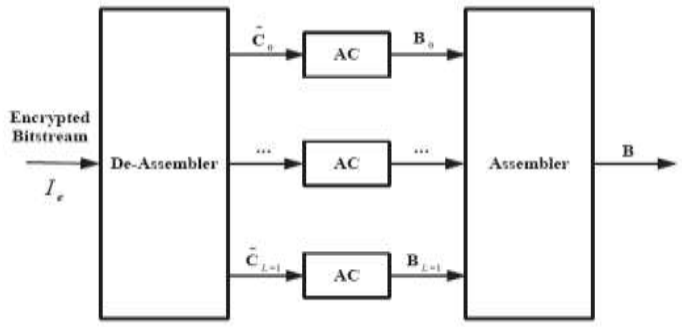


Fig. (4) Compressing the encrypted data. [1]

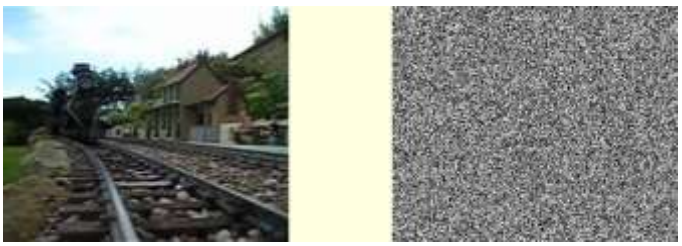
4.3. Arithmetic coding

Arithmetic coding is used for compression in binary data. It is quite useful in image and video compression. It works on probability distribution. The values used for any interval may be high or lov.lov is representing by 0 and high is representing by 1. We propose an image encryption scheme operated over the prediction and permutation based image encryption method and the efficiency of compressing the encrypted data [1]

4.4. Decryption and decompression

Decryption done by Bob using XOR of various decrypted clusters. As bob know the secret key so first of all he decrypt all the blocks and then calculates values of various cipher text and concatenate both values using XOR of all the blocks. The AC got de permutation and gives desired results.

5. Result and Performance Parameters.



(a) Original Image (b) Encrypted Image

Fig. 5 -Encryption

(a)Encrypted Image (b) Reconstructed Image

Fig. 6- Decryption

Table.1 Quality Measures of Image

The performance of given algorithm can be calculated by using following parameters.

Image	Performance Parameters			
Image Name	Compression Ratio	PSNR	Time elasped for encryption(Sec)	Time elapse for decryption(Sec)
1.Barbra	5.3329	30.303	56.388	45.882
2.Leena	4.7055	34.717	52.421	43.472
3.Saturans	4.6051	40.391	50.483	42.529
4.Peepers	4.1325	42.632	59.341	43.074
5.Boat	3.476	50.431	58.436	44.941
6.Baboon	6.663	47.497	56.497	42.873
7.Couple	5.037	46.952	59.032	43.643
8.Elina	5.492	43.325	64.953	52.376
9.Testpet	6.384	45.326	73.231	58.439
10.Terrace	5.943	42.251	70.359	61.360

5.1. Peak signal to noise ratio (PSNR)

The parameter is usually used to measure the quality of image. The parameter is widely used in image compression. It is a ratio between the maximum possible powers of signal to the power of corrupting noise which affect the fidelity. This caught the grey value difference between the result image and the input image. For good quality image this parameter should be high.

$$\text{PSNR}=\left[10\log\frac{255^2}{MSE}\right].$$

5.2. Mean squared error (MSE)

Simply error is the representation of degraded image. The error tells how the output image is different from the original image.MSE is the sum of all the square values difference to the image size and divided by three. Lower the value of this factor gives better result.

$$\mathbf{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

n=size (Input Image);

M=n (1);

N=n (2);

MSE = sum (sum ((Input Image- Reconstructed Image). ^2))/ (M*N);

6. CONCLUSION

In this paper we design a system that can provide features of both encryption and compression. The ETC system is based on clustering and random permutation. The encryption of image did by random error and clustering while that encrypted data can be compress using arithmetic coding. Arithmetic Coding based, Coding can't be cracked [1].so it provide a high level of security with a reasonable speed. The quality can be measure using tow parameters PSNR and MSE. For a good quality image the value of PSNR should be high and MSE should be low.

REFERENCES

[1] Jiantao Zhou,Xianiming Liu,Yuan Yan Tang,"Designing an efficient image encryption then compression system via prediction error clustering and random permutation" transaction on information forensics and security.vol.9.no.1.january 2014.

[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted Domain," IEEE Trans. Inf.

[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[4] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey- level and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.

[5]Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di,(2009)., "Digital image encryption algorithm based on chaos and improved DES",IEEE,international conference on system, man and cybernetics,2009

[6]Maitreyee Dutta,Parveen Kumar, "image encryption and compression using prediction error K mean clustering and cyclic permutation," International Journal of Advanced Research in Computer Science and management studies.Vol.3.April.2015

[7] Riyaz Sikander Kazi,Prof.Navnath Polkale, " Secure image transfer using clustering and permutation based approach", International Journal of Advanced Research in Computer Science and technology.Vol.4.june 2015.

[8] Ci-Lin Li, Chih-Yang Lin, and Tzung-Her Chen, "Efficient Compression-Jointed Quality Controllable Scrambling Method for H.264/SVC ", International Journal of Network Security, Vol.16, June 2014 .

[9] A.Shiva Krishna Reddy, K. Srimathi, R. Rajalakshmi, " Indexing Algorithm for Scrambled Frames in image Encryption " International Journal of Advanced Research in Computer Science and Software Engineering.Vol.4.Feb.2014.

[10] Yogita Negi, "A Survey on Video Encryption Techniques", International Journal of Emerging Technology and Advanced Engineering.Vol.3.April 2013.

[11] Wenjun Zeng1, Shawmin Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video", IEEE 2002.

[12] Amit Pande, Prasant Mohapatra, Joseph Zambreno, "Using Chaotic Maps for Encrypting Image and Video Content", IEEE International Symposium on Multimedia, 2011.

[13] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based for Image Encryption", World Academy of Science, Engineering and Technology , 2007.

[14] Jolly shah and Dr. Vikas Saxena, "Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, March 2011

[15] Preeti GuptA, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Vol 3, September 2012.

[16]Akanksha Mathur, "An ASCII value based data encryption algorithm and its compression with other symmetric data encryption algorithms, International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 4 No. 09 Sep 2012

[17]Daundkar Anita Mohan, Pratima Bhati. "Improving Image compression system by Random Permutation," International Journal of advanced Research in Computer Science and software and Engineering, ISSN : 2277 128X, Vol. 4,Issue 11, Nov 2014

[18]Pratibha S.Ghode, Abha Gaikwad, "A keyless approach to lossless image encryption" International Journal of advanced Research in Computer Science and software and Engineering, ISSN : 2277 128X, Vol. 4,Issue 5, may 2014

[19]Kalyani G.Nimborkar "Clustering and permutation based image encryption and compression system"International journals of research in advent technology, ISSN: 2321-9637, March 2015

[20] Behrouz A Forouzan, Data communication and networking. New York: McGraw-Hill, 2010.